SOC Compliance Explained: A Complete Guide for SaaS Companies 2025

SOC 2 Type I vs Type II: What's the Difference and Which is Right for You?

By 2025, SaaS companies will be growing at an unprecedented speed, and customer trust protection and data privacy matters more now than ever before. In the world's current economy, System and organization controls (SOC compliance) specifically SOC 2 compliance has become the gold standard for assessing how service provides to manage customer data. However, when companies initially think about **SOC 2 compliance**, a common thought comes into play... what's the difference with SOC 2 Type I vs Type II and which do I even care about first?

SOC 2 Type I

The SOC 2 Type I audit examines your security controls to see whether they are appropriately established at a given moment to satisfy the trust service requirements of security, availability, processing integrity, confidentiality, and privacy.

Best for: early-stage SaaS or startup businesses that are looking for quick trust signalling with prospects.

Key points:

- Point in time audit

- Shorter completion time (2-3 months)
- Reflects intent and planning of secure system

SOC 2 Type II

Conversely, SOC 2 Type II assesses your controls' operational efficacy across a time frame, usually three to twelve months.

Best suited for: Well-established SaaS organizations and those looking to offer enterprise client services.

Key characteristics:

- Observation over time
- Shows real-world effectiveness
- More believable for prospecting purposes, especially if you are in a regulated industry

What Should You Choose?

If you are just getting started and want to do something quickly to show you have an interest in practicing good security hygiene, start with SOC 2 Type I. But if you are looking to sell to enterprises or global clients, they will expect Type II. Most SaaS companies start with Type and go to Type II.

A Complete Checklist for Preparing for SOC 2 Audits

Passing the audit is only one aspect of SOC 2 compliance; another is developing a solid, safe, and dependable solution. Here is a list of **SOC 2 compliance checklist** requirements for SaaS companies in 2025.

Step 1: Phase of Scope

Identify which of the five Trust Service Criteria apply to your organization:

- Security (required)
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Tip: Most SaaS products will start with Security and Availability.

Step 2: Choose a Report Type

Determine if a SOC 2 Type I or SOC 2 Type II will suffice based on your growth stage and the expectations of your clients.

Step 3: Perform a Readiness Assessment

Before the audit, conduct a gap analysis to see your level of preparedness:

- Identify policies you are missing
- Assess your system configurations
- Interview stakeholders
- Test common security incidents

Outcome: a deliverable documenting the action plan to prepare for the audit.

Step 4: Apply Controls

Use platforms such as GRC (Governance, Risk & Compliance), or compliance automation software to apply controls for access control/user provisioning, vulnerability management, change management, incident response and security training/awareness programs.

Step 5: Document Take Everything

SOC audits tend to be documentation heavy. Keep records of:

- Security policies
- System architectural diagrams
- Risk assessments
- Audit trails and logs
- Onboarding/offboarding

Step 6: Train Your Team

Every team member should understand basic security hygiene. Conduct regular training sessions with your employees, covering such topics as:

- Phishing foods/social engineering
- Secure password practices
- Incident reporting procedures

Step 7: Perform Internal Audits

Before you proceed to the actual auditors, run an internal SOC 2 audit. Think of some of the typical audit questions and see how your systems and people would respond.

Step 8: Set Up a Licensed CPA Firm

The only valid SOC 2 report can be issued by a licensed CPA. Select a firm that has experience in a SaaS or cloud-native environment.

Top Companies That Help You Achieve SOC 2 Compliance

As SaaS companies scale in 2025, SOC 2 compliance has become a critical trust signal — not only for enterprise clients but also for investors and regulators. For many growing businesses, navigating SOC 2 requirements internally can be time-consuming, expensive, and complex.

1. CyberSigma – Your End-to-End SOC 2 Compliance Partner

CyberSigma is a consulting firm that specializes in cybersecurity that's tailored for today's modern SaaS businesses. Our focus on security, scalability, and compliance with the industry sets us apart in our ability to provide a hands-on and tailored journey to SOC 2.

Why CyberSigma is the Best:

End-to-End SOC 2 Expertise: CyberSigma covers the entire readiness, mapping, and audit phases and everything in between.

Built for SaaS: We understand SaaS businesses in fast-paced development environments and help them understand how to add security controls without slowing down.

Audit-Ready Documentation: CyberSigma supports companies with policies, evidence, and process and system mappings consistently documented and agreed to with the audit in mind.

Trusted by Growing Teams: We have the privilege of working with startups, mid-market platforms, and product-led companies who are growing at an incredibly fast pace on a global scale.

Human + Tech: We use some of the best tools in the industry and couple them with real expert guidance, so there are no cookie-cutter playbooks.

Whether you are preparing for a Type I or wanting to get on the path to Type II, CyberSigma provides you with the strategic support you need to get compliant faster - and smarter.

2. Vanta

Vanta is a prominent automated compliance platform providing tools to manage and monitor security controls on a continuous basis for SOC 2, ISO 27001, etc. It is a well-fit choice for tech- savvy teams looking for evidence collection based on integrations.

Strengths:

- Integrations (AWS, GitHub, G Suite, etc.) automation
- Continuous real-time compliance monitoring
- Partnership with audit firms for seamless transitions

3. Drata

Drata is another fast-growing compliance automation platform designed to better automate the SOC 2 compliance journey. With automated control mapping and real-time reporting, it would be particularly useful for DevSecOps teams needing automation.

Strengths:

- Continuous control monitoring

- Clean audit trails and dashboards

- Easily scalable as SaaS teams grow

4. Secureframe

Secureframe is an all-in-one compliance tool that combines compliance management together for SOC 2, ISO, HIPAA, GDPR, and more – everything lives within one platform. The support provided includes various templates, workflows, and relationships with auditors.

Strengths:

Easy-to-use platform for small-to-mid sized teams

Since they have so many policy templates to use, as well as support for onboarding teams, Secureframe can best assist early-stage compliance teams.

5.A-LIGN

A-LIGN is a cybersecurity and audit firm offering SOC 2 audits and advisory services. Unlike some platforms, they have significant expertise from a certified audit firm and can provide hands-on guidance.

Strengths:

- End-to-end audit services
- Experience with enterprise compliance
- Again, as a traditional audit firm, they have credibility

6. KPMG, BDO, EY and Deloitte

The Big Four and mid-tier audit firms provide SOC 2 Reporting under their assurance services. They are an appropriate option for mature organizations that want to work with a high trust audit partner.

Strengths:

- Global recognition and trust
- Strong audit capabilities
- Most organizations that are large typically use these firms as their audit service provider

How CyberSigma Supports Your SOC 2 Compliance

CyberSigma isn't a compliance consultant only. We are a strategic partner to help you build a scalable, security-first SaaS business.

Here are some of the ways in which we accelerate and simplify your SOC 2 journey:

1. **Tailored Readiness Assessment**

We start with an in-depth assessment of your current environment and gaps in policies, technical controls and documentation. Our experts will work with you to define what scope and Trust Service Criteria (TSC) you will need for your product and market.

2. **Implementation Support**
   We support you in implementing the required controls for SOC 2 without getting in the way of your business. We do everything from building access controls to helping you build incidence response plans.
3. **Documentation & Evidence Management**
   SOC 2 has a lot of documentation. We help you to bring everything an auditor will require in a single area, including policies, logs, workflows, evidence, etc., all in the formats that auditors would like to see, readily accessible.
4. **Auditor Communication Coordination**
   We will communicate and work with certified CPA firms on your behalf, coordinating communication with them to help facilitate evidences hand over and clarifying any technical questions, producing a smoother and more predictable audit process.
5. **Built for SaaS Scale**
   Our service works whether you are pre-Series A or post-Series A. I mean it when I say we are built to fit the changing nature of a SaaS business. We help you align compliance while growing your business model, not hold it back.

Source link